Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

10.__ USE OF U.S. CONTRACTORS FOR INSTALLATION AND MAINTENANCE OF SECURE TELECOMMUNICATIONS SYSTEMS

Reference: USCSB 12-13 "National Policy on Authorizing U.S. Contractor Access to Classified Federal Telecommunications or Communications Security Material"

A. The purpose of this Order is to clarify the procedures used to control contractor personnel access to classified information when contract services are required to install or maintain secure telecommunications systems.

1. The use of contractor personnel by the Agency for installation and maintenance of secure telecommunications systems which concentrate large volumes of classified, compartmented, or sensitive information should be considered only when there is no practical alternative.

2. Contractor personnel who perform installation or maintenance shall be U.S. citizens and must have the equivalent of a staff employee clearance and, where required, compartmented access approvals. The level of clearance should be equivalent to the classification level of the traffic passing through the system on which the contractor personnel are working.

3. The Agency will authorize limited access to classified traffic by U.S. contractors if such access is required for

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

the purpose of installing or maintaining secure telecommunications systems when it is in the best interest of the U.S. Government.

4. When contractor personnel require access to classified plain text (analog or digital) in order to perform their duties, their activities shall be monitored. In areas where there is a high concentration of classified traffic (MAX, ACT, Red Telephone switch), their work shall be conducted in the presence of appropriately-cleared, technically-competent staff employees. In areas where there is a limited amount of classified data available (IDF closets), contractor employee activities shall be periodically checked. When contractor personnel are working on the installation of secure systems or subsystems which are not operationally in use, they need not be as closely monitored. In every case, their work should be thoroughly checked before the system or subsystem is put to operational use.

5. Each component must make a reasonable and prudent effort to restrict access to only that classified information necessary for the contract employee to perform his duties. Uncontrolled access to files or recordings is not authorized. Good visitor control procedures and instructions to the contractor personnel must be established and maintained to fulfill the intent and purpose of this instruction.

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

6. Exceptions to the above shall be considered only when required by unique or urgent situations and must be expressly approved by the Director of Communications.

B. These criteria will be used in dealing with the Office of Security and the Office of Logistics in areas of joint organizational responsibilities. COTR's should insure that the clearance requirements are included in contracts of this nature.

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

USCSB 12-13

NATIONAL POLICY ON AUTHORIZING U.S. CONTRACTORS ACCESS TO CLASSIFIED FEDERAL TELECOMMUNICATIONS OR COMMUNICATIONS SECURITY MATERIAL

United States
Communications Security Board

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

USCSB
UNITED STATES
COMMUNICATIONS
SECURITY BOARD

FOREWORD

This policy was approved by the United States Communications Security Board in October 1973 and supersedes the policies issued under:

USCSB 13–201A, National Policy on Utilization of Contractor Personnel in U.S. Government Secure Telecommunications Operations, dated 3 February 1969.

USCSB 13–201B, National Policy on the Provision of Crypto-Equipment or Other COMSEC Material to U.S. Industrial Organizations, dated 3 February 1969.

USCSB 9–13, National Policy on the Release of Specified Communications Security Systems to Contractor Personnel, dated 23 July 1972.

This policy recognizes the increasing dependence of the Government on U.S. commercial contractors to install, operate, and maintain sophisticated secure telecommunications systems and provides for such use of contractors. It also recognizes the need for the Heads of the U.S. Government departments and agencies to be able to authorize the release and provision of manual COMSEC systems to contractors for use in U.S. Government secure telecommunications systems.

The policy delegates authority from the USCSB to the Heads of U.S. Government departments and agencies to release COMSEC material to U.S. industrial firms under contract to the U.S. Government and stipulates the conditions under which release is permissible.

Provisions have been made herein for obtaining exceptions to this policy.

In this revised policy, the citizenship requirement (Section V) has been modified so that contractor personnel must be appropriately cleared U.S. citizens *only* if they will have access to classified COMSEC information or material.

Implementation of this policy is the responsibility of individual departments and agencies.

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

NATIONAL POLICY ON AUTHORIZING U.S. CONTRACTORS ACCESS TO CLASSIFIED FEDERAL TELECOMMUNICATIONS OR COMMUNICATIONS SECURITY MATERIAL

31 October 1973

Section I—Purpose

1. This document provides national policy for:

a. Authorizing limited access by U.S. contractors to classified Federal telecommunications when contractor installation, maintenance, or operation of U.S. Government secure telecommunications systems is required.

b. Providing cryptographic equipment or other COMSEC material to U.S. contractors for:

(1) Research, development, production, and testing of cryptographic equipment, or equipment interfacing with cryptographic equipment, being undertaken on behalf of the U.S. Government.

(2) Protection of information related to classified contracts, which is either generated by a contractor or provided by the U.S. Government, and which must be transmitted electrically among contractors, or between contractors and the U.S. Government.

c. Providing manual COMSEC systems to U.S. contractors. Contractors may use manual COMSEC systems to protect classified information in telecommunications systems which the contractors operate on behalf of the U.S. Government, or to protect classified information relating to U.S. Government contracts which must be transmitted electrically between contractors or between the contractor and the U.S. Government.

Section II—Background

2. From the standpoint of security and control of operations during both normal and emergency conditions, the installation, maintenance, and operation of U.S. Government secure telecommunications systems should be performed by appropriately cleared U.S. citizens, who are military or civilian employees of the U.S. Government. However, with the continuing trend toward more complex and automated secure telecommunications systems, greater involvement of industry and more dependence on highly-skilled contractor personnel can be expected. Personnel involved may thereby require some degree of access to the classified information processed through such systems, although the need-to-know the information exists only in order to assure proper functioning of the system.

3. For specific purposes in the conduct of government business, there is a continuing need to provide cryptographic equipment and other COMSEC material and information to certain industrial organizations. These purposes include the production and testing of equip-

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

ment and the safeguarding of sensitive information being transmitted electrically between contractors or between the contractor and the U.S. Government.

Section III—Scope

4. The provisions of this policy apply to all departments and agencies of the Federal Government which permit limited access by contractor personnel to U.S. classified telecommunications or which provide COMSEC information or material to U.S. contractors.

Section IV—Policy

5. The heads of the departments and agencies of the U.S. Government may authorize limited access to U.S. classified traffic by U.S. contractors or may authorize the release of COMSEC information or material to U.S. contractors for any of the stated purposes when such releases are judged to be in the best interests of the U.S. Government. Certain requirements must be met to insure that uniform procedures and safeguards are applied to releases.

Section V—Requirements

6. Certain requirements must be met if contractor personnel:

a. Have any access to U.S. Government classified traffic or operational cryptographic keying material, or,

b. Install, maintain, or operate cryptographic equipment for the U.S. Government, or,

c. Use manual COMSEC systems, or,

d. Have access to classified COMSEC information or material.

7. These requirements are as follows:

a. Such contractor personnel shall be U.S. citizens cleared by the U.S. Government to the level required by the contract, based on the security classification of the information or material involved. The clearance required for functions outlined in *6a* and *6b* shall be based on a full-field investigation. The investigation shall be updated and the security clearance reviewed at intervals not to exceed five years.

b. Operations and maintenance of secure telecommunications systems for the purpose outlined in paragraph 1*a* shall be conducted in the presence of appropriately cleared, government civilian employees or military personnel. The functions outlined in 1*b* and 1*c* need not be performed in the presence of government personnel.

8. Contractor personnel shall be permitted access only to that COMSEC information and material which is directly necessary in the performance of their contractual functions.

9. The contracting U.S. Government department or agency shall insure that all applicable rules, regulations, and doctrine contained in operating, maintenance, and general cryptographic and COMSEC publications are met.

10. Contractor personnel shall be given security briefings by the U.S. Government in the same manner and frequency as established for U.S. Government personnel, but not less frequently than annually. In addition to covering general security responsibilities, the

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

briefings shall stress the requirement that any information (classified, administratively controlled, or unclassified) acquired as a result of their U.S. Government contractual functions is official U.S. Government information and is not to be disclosed without the specific approval of the cognizant U.S. Government authority.

11. The contract shall provide for a standard of physical security for COMSEC information or material at least equivalent to that prescribed by USCSB Policy 1–7, National Policy for the Control of Communications Security Material, dated 1 August 1973. Security standards shall be consistent with appropriate industrial security regulations (i.e., DOD Industrial Security Manual for Safeguarding Classified Information, DOD 5220.22–M, and the COMSEC Supplement [5220.22–S] thereto) and pertinent U.S. Government department or agency security regulations. The contract shall specifically require that classified information acquired by contractor personnel in the performance of their contractual functions shall be handled within the contractor organization in strict accordance with need-to-know procedures as established by the cognizant U.S. Government authority.

12. COMSEC material used in the electrical transmission of classified information shall be limited to that which has been approved by the Director, National Security Agency, for U.S. Government use.

13. Departments and agencies of the U.S. Government shall advise the USCSB of each instance in which contractor personnel are used to operate or maintain a secure telecommunications system on behalf of the U.S. Government, and of the termination of such arrangements. *Whenever possible, advance notification should be given to the USCSB.*

14. Each U.S. Government department and agency shall provide the Director, National Security Agency, with a report of all instances of the provision of operational COMSEC material to contractors for use in the transmission of classified information, and the termination thereof. The Director, National Security Agency, shall maintain records of all such reported releases and annually shall advise the USCSB, by 1 March, of the status of contractor use of COMSEC material.

Section VI—Exceptions

15. In the event that any requirement of this policy cannot be met, approval of the USCSB shall be obtained *prior* to the employment of contractors. Requests for USCSB approval of exception, with justification and explanatory details, shall be forwarded to the USCSB through the Director, National Security Agency, who shall provide appropriate recommendations for USCSB consideration.

Approved For Release 2001/04/09 : CIA-RDP79-01577A000100040006-1

Approved For Release 2001/04/09 : CIA-RDP78-01577A000100040006-1

SENDER WILL CHECK CLASSIFICATION TOP AND BOTTOM

UNCLASSIFIED | CONFIDENTIAL | SECRET

OFFICIAL ROUTING SLIP

TO	NAME AND ADDRESS	DATE	INITIALS
1	D/CO		
2			
3			
4			
5			
6			

	ACTION		DIRECT REPLY		PREPARE REPLY
	APPROVAL		DISPATCH		RECOMMENDATION
	COMMENT		FILE		RETURN
	CONCURRENCE		INFORMATION		SIGNATURE

Remarks:

This is a draft OC Order which is one of the agenda items for the Executive Board Meeting this afternoon.

Please bring this copy to the meeting.

FOLD HERE TO RETURN TO SENDER

FROM: NAME, ADDRESS AND PHONE NO.	DATE
Chief, OC-CS/604 Mag/2418	9 July 74

UNCLASSIFIED | CONFIDENTIAL | SECRET

Approved For Release 2001/04/09 : CIA-RDP78-01577A000100040006-1

FORM NO. 237 Use previous editions (40)
1-67